



- **Multi-Core Performance-Architektur**
- **Unified Threat Management-Sicherheitsplattform**
- **Flexible Implementierung**
- **Application Firewall und benutzerspezifische Überwachungsfunktionen**
- **Dynamischer Schutz**

Schutz und Performance

Mit der SonicWALL® E-Class Network Security Appliance (NSA)-Serie präsentiert SonicWALL die weltweit erste Multi-Core United Threat Management (UTM)-Lösung, die Enterprise-Class Deep Packet Inspection bietet, ohne den Netzwerkdurchsatz merklich zu beeinträchtigen. Die Appliance verbindet eine leistungsfähige Deep Packet Inspection-Firewall mit mehrstufigen Schutzmechanismen und zahlreichen Hochverfügbarkeitsfunktionen. Mit den E-Class NSA E7500-, E6500- und E5500-Appliances bietet SonicWALL ein breites Angebot an skalierbaren Lösungen für die verschiedensten Infrastrukturen wie etwa verteilte Netzwerke, Campus-Netzwerke und Rechenzentren.

Als hochskalierbare, leistungsstarke und zuverlässige multifunktionale Threat Appliances bieten die SonicWALL E-Class NSAs weit mehr als vergleichbare Lösungen ihrer Klasse. Die NSA-Serie schützt Unternehmensnetze nicht nur umfassend vor einer Vielzahl von Bedrohungen – sie bietet auch eine außergewöhnlich hohe Geschwindigkeit. Möglich wird dies durch ihre Multi-Core-Architektur, bei der mehrere Prozessorkerne parallel arbeiten und so extrem schnellen Schutz bei größtmöglicher Skalierbarkeit gewährleisten. Dem Administrator erschließen sich mit der Funktion Application Firewall völlig neue Dimensionen in puncto Schutz und Steuerung: Eine Reihe individuell anpassbarer Sicherheitstools ermöglicht eine detaillierte Kontrolle und Überwachung des Netzwerkverkehrs. Verschiedene Hochverfügbarkeitsfunktionen auf der Hardware- und Systemebene sorgen für einen zuverlässigen Betrieb, reduzieren Ausfallzeiten auf ein Minimum und verbessern den Netzwerkschutz.

Die NSA-Serie ist ein wichtiger Bestandteil von SonicWALLs Enterprise-Class-Portfolio an Network Security-, E-Mail Protection- und Secure Remote Access-Produkten und -Services. Alle E-Class-Lösungen bieten größtmögliche Sicherheit und höchste Performance bei optimaler Benutzerfreundlichkeit und einem unschlagbaren Preis-Leistungs-Verhältnis. Die SonicWALL E-Class bietet Unternehmen mit Enterprise-Class-Netzwerken High-Performance Protection in einer Lösung, die einen sicheren Netzwerkbetrieb ermöglicht und dabei Kosten und Komplexität senkt.

Funktionen und Vorteile

Multi-Core Performance-Architektur. Das Herzstück der E-Class NSA bildet die SonicWALL Multi-Core Performance-Architektur. Sie sorgt für überragende Deep Packet Inspection und eine gezielte Überwachung des Echtzeit-Netzwerkverkehrs, ohne dass die Performance beeinträchtigt wird. Durch den gleichzeitigen Einsatz von spezialisierten Security-Prozessor-Cores bietet die SonicWALL E-Class NSA eine extrem schnelle Performance. Die gebündelte Rechenpower mehrerer Prozessorkerne steigert die Durchsatzrate sowie die Effizienz der Deep Packet Inspection, während gleichzeitig der Verwaltungsaufwand reduziert wird.

Unified Threat Management-Sicherheitsplattform.

Mit der E-Class NSA-Serie steht Unternehmen eine hochredundante Netzwerk- und Sicherheitsplattform zur Verfügung, die für High-Speed-Netzwerkschutz vor internen und externen Bedrohungen sowie für die Konsolidierung und Erweiterung der Sicherheitsfunktionen im gesamten Netzwerk ausgelegt ist. Die E-Class NSAs vereinen Gateway Anti-Virus, Anti-Spyware und Intrusion Prevention in Echtzeit und schützen so das Netzwerk vor einer Vielzahl dynamischer Bedrohungen wie etwa Würmern, Trojanern, Viren, Malware und Software-Schwachstellen.

Flexible Implementierung. Die E-Class NSA Appliances sind für einen hochredundanten Betrieb ausgelegt und eignen sich optimal für kabelgebundene oder drahtlose Anwendungen, die einen High-Speed-Zugang und eine

starke Segmentierung von Arbeitsgruppen erfordern. Dank integriertem Support für standardisierte VoIP-Funktionen sowie Virtual Local Area Networks (VLANs), Enterprise-Class-Routing und QoS-Features gewährleisten die E-Class NSAs eine flexible Implementierung und tragen dazu bei, die Mitarbeiterproduktivität zu erhöhen.

Application Firewall und benutzerspezifische Überwachungsfunktionen.

Die Application Firewall umfasst eine Reihe konfigurierbarer, granularer und anwendungsspezifischer Regeln, die eine individuelle Zugriffssteuerung nach Netzwerknutzern, Anwendungen, Zeitplänen oder IP-Subnetzen erlauben. Anhand dieser Regeln lassen sich Transfers bestimmter Dateien und Dokumente einschränken, E-Mail-Anhänge anhand benutzerdefinierter Kriterien scannen, die Bandbreite automatisch überwachen, der Webzugriff von internen wie externen Benutzern verwalten sowie kundenspezifische Signaturen erstellen.

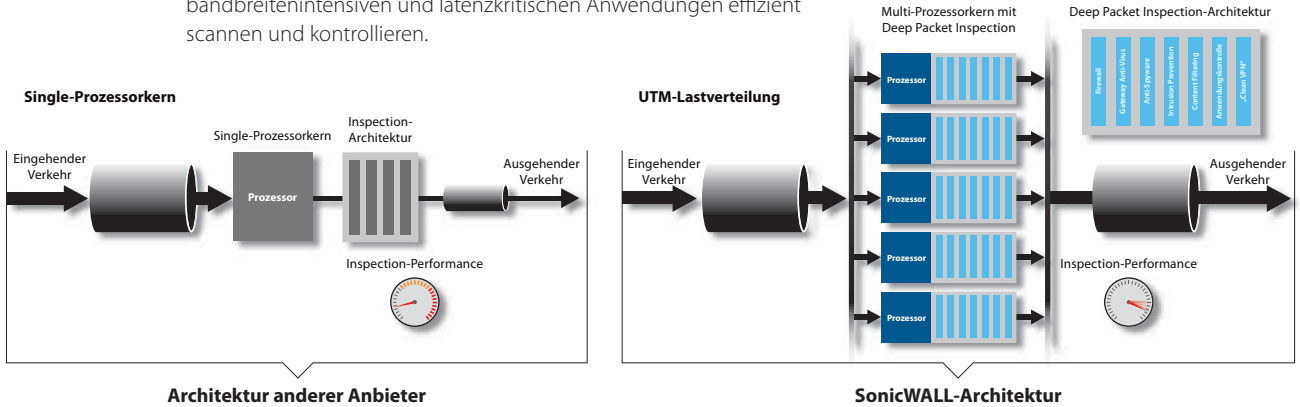
Dynamischer Schutz. Dynamic Threat Protection, Content Filtering sowie Funktionen zur Anwendungssteuerung werden rund um die Uhr aktualisiert, um größtmögliche Sicherheit bei überschaubaren Kosten zu gewährleisten. Da die Verwaltung von Ad-hoc-Patches für Server und Arbeitsstationen entfällt, neue Schutzsignaturen automatisch angewendet werden und die Sicherheitsregeln nicht manuell aktualisiert werden müssen, können IT-Mitarbeiter produktiver arbeiten.

E-Class Network Security Appliance-Architektur

Integrierter, erstklassiger Schutz vor Sicherheitsbedrohungen

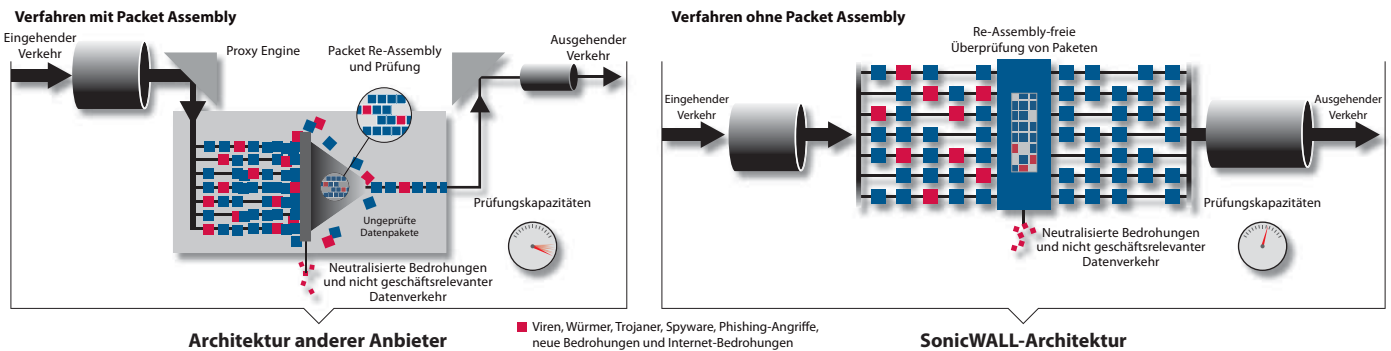
Unified Threat Management-Lastverteilung

Lösungen, die mit unterschiedlichen Sicherheitstechnologien arbeiten, aber nur über einen zentralen Prozessor verfügen, sind in ihrer Leistung deutlich eingeschränkt. Bei der UTM-Lastverteilung von SonicWALL dagegen werden Anwendungen, Dateien und contentbasierter Datenverkehr in Echtzeit von einer High-Speed Deep Packet Inspection- und Traffic Classification-Engine geprüft, die auf mehreren Sicherheits-Cores integriert ist – ohne dabei Performance und Skalierbarkeit merklich zu beeinträchtigen. Dadurch lassen sich Sicherheitsbedrohungen in Enterprise-Class-Netzen mit bandbreitenintensiven und latenzkritischen Anwendungen effizient scannen und kontrollieren.

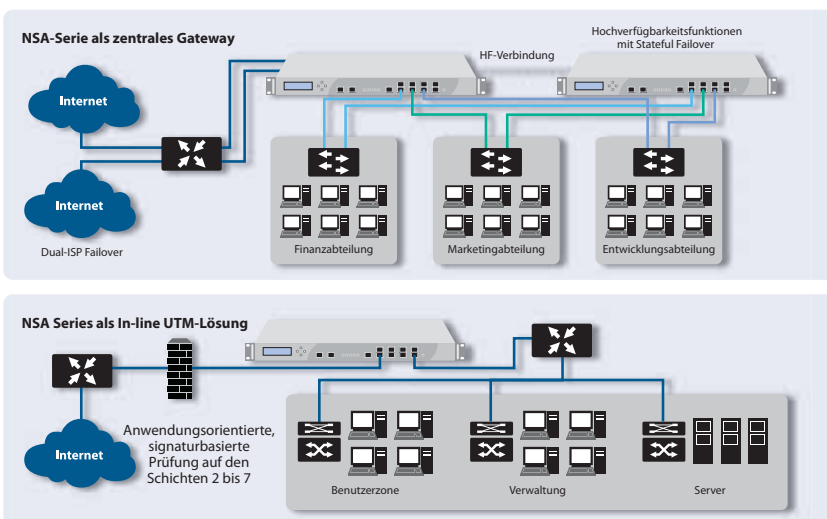


Unified Threat Management-Engine

Als erste skalierbare Inspection Engine für die Anwendungsebene kann die SonicWALL E-Class NSA UTM-Engine unbegrenzt große Dateien und Inhalte in Echtzeit analysieren, ohne dass dafür die Datenpakete oder der Content wieder zusammengesetzt werden müssen. Diese Methode wurde speziell für Echtzeit-Anwendungen und latenzkritischen Datenverkehr konzipiert und erlaubt eine umfassende Kontrolle und Prüfung des Netzwerkverkehrs, ohne dabei Proxyverbindungen einsetzen zu müssen. Auf diese Weise lässt sich High-Speed-Netzwerkverkehr nicht nur effizienter, sondern auch zuverlässiger prüfen.



Flexible und individuelle Implementierungsoptionen



Zentrales Gateway

Als zentrales Gateway implementiert die NSA-Serie eine skalierbare Hochgeschwindigkeitsplattform mit VLANs und Sicherheitszonen für Netzwerksicherheit und – Segmentierung. Außerdem verfügt die NSA-Serie über Redundanzfunktionen wie z. B. WAN-Lastverteilung, ISP Failover und Hochverfügbarkeitsfunktionen mit Stateful Failover.

Layer 2 Bridge-Modus

Der Layer 2 Bridge-Modus verfügt über ein Inline Intrusion Detection System und eine zusätzliche zonenbasierte Sicherheitsschicht für Netzwerksegmente oder Geschäftsbereiche und verringert so die Komplexität der Multi-Layer-Sicherheitslösung. Außerdem können Administratoren auf diese Weise den Zugriff auf sensible Daten nach bestimmten Geschäftsbereichen oder Datenbank-Servern einschränken.

Mehrschichtiger Schutz

Effizienter Schutz für Remote-Standorte

Die E-Class NSA-Serie bietet Ultra-High-Performance VPNs, die sich problemlos für tausende von Endpunkten und Zweigstellen skalieren lassen. Die innovative SonicWALL Clean VPN™-Technologie säubert den Datenverkehr in Echtzeit und ohne Benutzer-Eingriff, bevor dieser das Unternehmensnetzwerk erreicht. Auf diese Weise werden Sicherheits-schwachstellen und bösartiger Code neutralisiert.

Gateway-Schutz

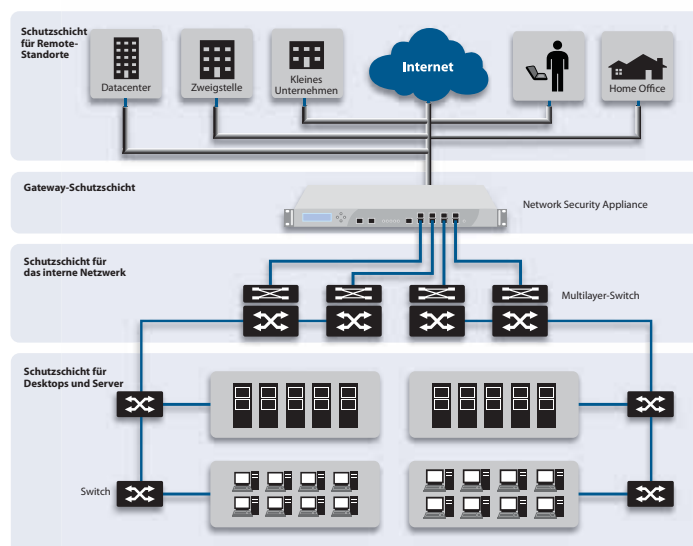
Die E-Class NSAs lassen sich leicht in bestehende Umgebungen integrieren und bieten einen zentralisierten Gateway-Schutz für alle eingehenden und ausgehenden Anwendungen und Dateien sowie für den contentbasierten Datenverkehr. Gleichzeitig überwachen die E-Class NSAs Anwendungen und Bandbreite, ohne die Performance oder Skalierbarkeit zu beeinträchtigen.

Interner Schutz

Mit einer Vielzahl unterschiedlicher Konfigurationsoptionen ausgestattet, prüft die E-Class NSA-Serie auch den Datenverkehr über LAN-Schnittstellen und VLANs und dehnt so den Netzwerkschutz auf das interne Netzwerk aus. Die speziell für LAN-Netzwerkbedrohungen konzipierte E-Class NSA-Serie überwacht und reagiert auf Malware, DoS-Angriffe, Bedrohungen durch Sicherheitslücken, Regelverletzungen, vertrauliche Dokumente und den Missbrauch von Netzwerkressourcen innerhalb des internen Netzwerks.

Desktop- und Server-Schutz

Dank ihres Anti-Virus- und Anti-Spyware-Clients mit heuristischer Analyse bietet die E-Class NSA-Serie neben den Netzwerk- und Gateway-basierten Sicherheitsfunktionen außerdem einen zusätzlichen Endpunkt-Schutz für Arbeitsstationen und Server. Diese automatisierte Client-Lösung kontrolliert den Netzwerkzugriff, indem sie nur Endpunkten mit den neuesten Signaturen oder Engine-Updates den Zugang zum Internet erlaubt. Ist die Enforcement-Funktion der Appliance aktiviert, wird jeder Endpunkt angewiesen, den Enforced Anti-Virus and Anti-Spyware Client herunterzuladen, ohne dass ein



Administrator eingreifen muss. Auf diese Weise wird die Implementierung von Endpunkt-Sicherheitsfunktionen automatisiert.

Zentralisierte Regelverwaltung

Das SonicWALL Global Management System (GMS) bietet flexible, leistungsstarke und intuitive Tools, um die E-Class NSA-Serie in verteilten Unternehmensnetzwerken zentral zu verwalten und zu konfigurieren. Darüber hinaus lassen sich mit GMS Überwachungsdaten in Echtzeit anzeigen und Regel- bzw. Compliance-Berichte erstellen.



Abo-Services

Jede E-Class-Network Security Appliance unterstützt eine wachsende Anzahl von dynamischen Abo-Services und Softwarelösungen, die sich nahtlos in jedes Netzwerk integrieren lassen.



Gateway Anti-Virus/Anti-Spyware/Intrusion Prevention Service von SonicWALL bietet umfassenden Echtzeit-Netzwerkschutz gegen komplexe Angriffe über die Anwendungsebene und contentbasierte Angriffe (z. B. Viren, Spyware, Würmer, Trojaner sowie Software-Schwachstellen wie Pufferüberläufe).



Enforced Client and Server Anti-Virus and Anti-Spyware bietet Laptops, Desktop-PCs und Servern umfassenden Viren- und Spyware-Schutz mittels eines einzigen integrierten Clients. Anti-Virus- und Anti-Spyware-Regeln sowie Definitionen und Software-Updates werden automatisch im gesamten Netzwerk angewendet.



Content Filtering Service setzt eine innovative Rating-Architektur ein, die maximalen Schutz vor anstößigen Webinhalten und privatem Surfen bietet. Mithilfe einer dynamischen Datenbank werden über 55 Kategorien von unerwünschtem Web-Content blockiert.



ViewPoint von SonicWALL ist ein komfortables webbasiertes Reportingtool, das detaillierte Informationen über die Performance und Sicherheit liefert. Historische Reports auf der Grundlage von Übersichten und detaillierten Zusammenfassungen unterstützen große und kleine Organisationen bei der Kontrolle der Internetnutzung, bei der Einhaltung gesetzlicher Vorschriften sowie bei der Überwachung der Netzwerksicherheit.



SonicWALL E-Class 24/7-Support Der speziell für E-Class-Kunden konzipierte E-Class 24/7-Support bietet Support-Funktionen und Servicequalität der Enterprise-Klasse. Der E-Class 24/7-Support umfasst telefonischen und webbasierten technischen Support rund um die Uhr, an 365 Tagen im Jahr, sowie direkten Kontakt mit einem Team hervorragend ausgebildeter und erfahrener Support-Ingenieure. Hinzu kommen Software- und Firmware-Updates bzw. -Upgrades, Vorabaustausch von Hardware, Zugriff auf elektronische Support-Tools, moderierte Diskussionsgruppen und vieles mehr.

Technische Daten

Artikelnummern für die E-Class NSA-Serie



SonicWALL NSA E7500
01-SSC-7000



SonicWALL NSA E6500
01-SSC-7004



SonicWALL NSA E5500
01-SSC-7008

SonicWALL NSA E7500 Security Services

SonicWALL Content Filtering Service Premium Business Edition für die NSA E7500 (1 Jahr)
01-SSC-7329
SonicWALL GAV / IPS / Application Firewall für die NSA E7500 (1 Jahr)
01-SSC-6130
SonicWALL Comprehensive Gateway Security Suite für die NSA E7500 (1 Jahr)
01-SSC-6120
SonicWALL E-Class Support 24/7 für die NSA E7500 (1 Jahr)
01-SSC-7254

SonicWALL NSA E6500 Security Services

SonicWALL Content Filtering Service Premium Business Edition für die NSA E6500 (1 Jahr)
01-SSC-7330
SonicWALL GAV / IPS / Application Firewall für die NSA E6500 (1 Jahr)
01-SSC-6131
SonicWALL Comprehensive Gateway Security Suite für die NSA E6500 (1 Jahr)
01-SSC-6121
SonicWALL E-Class Support 24/7 für die NSA E6500 (1 Jahr)
01-SSC-7257

SonicWALL NSA E5500 Security Services

SonicWALL Content Filtering Service Premium Business Edition für die NSA E5500 (1 Jahr)
01-SSC-7331
SonicWALL GAV / IPS / Application Firewall für die NSA E5500 (1 Jahr)
01-SSC-6132
SonicWALL Comprehensive Gateway Security Suite für die NSA E5500 (1 Jahr)
01-SSC-6122
SonicWALL E-Class Support 24/7 für die NSA E5500 (1 Jahr)
01-SSC-7260

Lizenzen auch für mehrere Jahre erhältlich. Weitere Informationen unter www.sonicwall.com/de

	NSA E5500	NSA E6500	NSA E7500
Firewall			
SonicOS-Version	SonicOS Enhanced 5.0 (oder höher)		
Stateful-Durchsatz¹	2 GBit/s	3 GBit/s	5,5 GBit/s
GAV-Performance²	750 MBit/s	900 MBit/s	1,8 GBit/s
IPS-Performance²	550 MBit/s	850 MBit/s	1,2 GBit/s
UTM-Performance-Durchsatz	400 MBit/s	750 MBit/s	1 GBit/s
Maximale Verbindungen	700.000	750.000	1.000.000
Neue Verbindungen/Sekunde	10.000	19.000	25.000
Unterstützte Nodes	Unlimitiert		
Schutz vor Denial of Service-Angriffen	22 Kategorien von DoS-, DDoS- und Scan-Angriffen		
VPN			
3DES/AES-Durchsatz¹	1,5 GBit/s	2,5 GBit/s	4 GBit/s
Site-to-Site VPN-Tunnel	4.000	6.000	10.000
Gebündelte Global VPN Client-Lizenzen für Remote Access	2.000	2.000	2.000
Verschlüsselung / Authentifizierung	DES, 3DES, AES (128, 192, 256-Bit)/MD5, SHA-1		
Schlüsselaustausch	IKE, IKEv2, manueller Schlüssel, PKI (X.509)		
L2TP/IPSec	Ja		
Unterstützte Zertifikate	Verisign, Thawte, Baltimore, RSA Keon, Entrust und Microsoft CA für SonicWALL-to-SonicWALL VPN		
Redundantes VPN-Gateway	Ja		
Unterstützte Global VPN Client-Plattformen	Microsoft® Windows 2000, Windows XP, Microsoft® Vista 32-Bit		
Deep Packet Inspection Security Services			
Deep Packet Inspection Signature Service	Umfassende Signaturrendatenbank (keine Server-Unterstützung). Signaturreupdates und Überwachung von Peer-to-Peer- und Instant Messaging-Anwendungen erfolgen über die Distributed Enforcement Architecture.		
Content Filtering Service (CFS) Premium Edition	Prüfung nach HTTP URL, HTTPS IP, Schlüsselwörtern und Content, Blockieren von ActiveX, Java Applets und Cookies		
Client Anti-Virus und Anti-Spyware am Gateway	HTTP/S, SMTP, POP3, IMAP und FTP, Installation von McAfee™-Clients, Blockieren von E-Mail-Anhängen		
Application Firewall	Umsetzung von Schutzmechanismen auf Anwendungsebene mit Bandbreitenkontrolle, Kontrolle von Internet-Verkehr, E-Mail, E-Mail-Anhängen und Dateitransfers, Scannen und Sperren von Dokumenten und Dateien nach Schlüsselwörtern und -phrasen		
Networking			
IP-Adresszuweisung	Statisch (DHCP-, PPPoE-, L2TP- und PPTP-Client), interner DHCP-Server, DHCP-Relay		
NAT-Modi	1:1, 1:many, many:1, many:many, flexible NAT (überlappende IPs), PAT, transparenter Modus		
VLAN-Ports (802.1q)	256	256	512
Routing	OSPF, RIPv1/v2, statische Routen, regelbasiertes Routing, Multicast		
QoS	Bandbreitenpriorität, maximale Bandbreite, garantierte Bandbreite, DSCP-Markierung, 802.1p		
Authentifizierung	XAUTH/RADIUS, Active Directory, SSO, LDAP, interne Benutzerdatenbank		
Benutzerdatenbank	1.500 User	2.500 User	2.500 User
VoIP	Voll H.323v1-5-kompatibel, SIP, Gatekeeper-Unterstützung, Verwaltung der ausgehenden Bandbreite, VoIP über WLAN, Deep Inspection Security, vollständige Interoperabilität mit den meisten VoIP Gateway- und Kommunikationsgeräten		
System			
Verwaltung und Überwachung	Web-Oberfläche (HTTP, HTTPS), Command Line (SSH, Konsole) SNMP v2; zentrale Verwaltung mit SonicWALL GMS		
Logging und Reporting	ViewPoint®, lokale Logdatei, Syslog		
Hochverfügbarkeit	Active/Passive mit State Sync		
Lastverteilung	Ja (abgehend mit prozentbasierter, Round-Robin- und Spillover-Lastverteilung; ankommend mit Round-Robin, zufälliger Verteilung, Sticky IP, blockweiser Neuordnung und symmetrischer Neuordnung)		
Standards	TCP/IP, UDP, ICMP, HTTP, HTTPS, IPsec, ISAKMP/IKE, SNMP, DHCP, PPPoE, L2TP, PPTP, RADIUS		
Wireless-Standards	802.11 a/b/g, WEP, WPA, TKIP, 802.1x, EAP-PEAP, EAP-TTLS		
Hardware			
Schnittstellen	(8) 10/100/1000 Kupfer-Gigabit-Ports, 1GbE HA-Schnittstelle, 1 Konsolenschnittstelle, 2 USB-Schnittstellen (für späteren Einsatz)	(8) 10/100/1000 Kupfer-Gigabit-Ports, 1GbE HA-Schnittstelle, 1 Konsolenschnittstelle, 2 USB-Schnittstellen (für späteren Einsatz)	1 Konsolenschnittstelle, 4 Gigabit-Ethernet-Schnittstellen, 4 SFP-Ports (Sx, Lx oder Tx), 1GbE HA-Schnittstelle, 2 USB-Schnittstellen (für späteren Einsatz)
Speicher (RAM)	1 GB	1 GB	2 GB
Flash-Speicher	512 MB Compact Flash	512 MB Compact Flash	16 MB, 512 MB Compact Flash
Stromversorgung	Single-250 W ATX-Stromversorgung	Single-250 W ATX-Stromversorgung	Dual-250 W ATX, hot-swappable
Lüfter	Dual-Lüfter, hot-swappable		
Display	Front-LCD-Display		
Eingangsspannung	100-240 VAC, 60-50 Hz		
Maximale Leistungsaufnahme	81 W	90 W	150 W
Wärmeabgabe	276 BTU	307 BTU	511,5 BTU
Ausstehende Zertifikate	ICSA IPsec VPN 1.0d, ICSA Firewall 4.1, FIPS 140-2 Level 2, EAL-4+		
Gehäuse	Rackfähig (1 HE)		
Abmessungen	43,2 x 42,5 x 4,4 cm		
Gewicht	6,80 kg	6,85 kg	7,9 kg
WEEE-Gewicht	6,80 kg	6,85 kg	7,9 kg
Erfüllt folgende Standards/Normen	FCC Class A, CES Class A, CE, G-Tick, VCCI, Compliance MIC, UL, cUL, TÜV/GS, CB, NOM, RoHS, WEEE		
Umgebungstemperatur	5-40°C		
Luftfeuchtigkeit	10-90 % nicht kondensierend		

¹Messung des Firewall- und VPN-Durchsatzes gemäß RFC 2544 bei UDP-Verkehr

²Messung des Gateway AV/Anti-Spyware/IPS-Durchsatzes mittels Industriestandard-HTTP Performance-Test WebAvalanche von Spirent

SonicWALL Deutschland

Tel.: +49 89 4545 946
www.sonicwall.de

SonicWALL Schweiz

Tel.: +41 44 810 31 35
www.sonicwall.ch

SonicWALL Österreich

Tel.: +41 44 810 31 35
www.sonicwall.at



PROTECTION AT THE SPEED OF BUSINESS™